FIRST
Improving Security Together

June 17–22, 2007
Melia Sevilla Hotel
Seville, Spain

SEVILLE JUNE2007 SPAIN
19th Annual **FIRST** Conference

Last updated: June 21st, 2007

Conference overview

Saturday, June 16th
Train the Trainers Workshop

Sunday, June 17th
Train the Trainers Workshop
Registration
Program Committee Meeting
Welcome Icebreaker Reception

Monday, June 18th
Tutorials
Geek Zone
SIG Meetings
Beer 'n Gear

Tuesday, June 19th
Tutorials
SIG Meetings
Pre-AGM

Wednesday, June20th
Keynote Speakers
Main Conference
Geek Zone
SIG Meetings
Vendor Booths
Conference Banquet

Thursday, June 21st
Keynote Speakers
Main Conference
Geek Zone
SIG Meetings
Vendor Booths
Annual General Meeting (AGM)
Sponsor Reception
Birds of a Feather (BOF) — Giralda III, Santa Cruz, Nervion I & II, Arenal I, Arenal/Nervion III

Friday, June 22nd
Keynote Speakers
Main Conference
Geek Zone
SIG Meetings
Vendor Booths
Conference Closing

Facilities

Registration – Triana Foyer

Sunday	14:00–18:00
Mon–Wed	08:00–17:00
Thu–Fri	08:00–14:00

Vendor Booths – Giralda IV & V

Wed–Fri	08:00–18:00

Terminal Room – Giralda VI & VII

Mon–Thu	08:00–17:00
Friday	08:00–14:00

Lunch – Restaurant

Mon–Fri	13:10–14:40

Sponsors

Supported by	enisa European Network and Information Security Agency
Diamond Sponsor	BT
Platinum Sponsor	CERT Software Engineering Institute Carnegie Mellon
Local Host and Gold Sponsor	RedIRIS
Gold & Beer 'n Gear Sponsor	Internet Security Systems, an IBM Company
Gold Sponsor	CCN-CERT
Gold Sponsor	citi
Gold Sponsor	enisa European Network and Information Security Agency
Gold Sponsor	"la Caixa"
Internet Sponsor	Telefonica
Network Sponsor	cisco
Silver Sponsor	inteco
Silver Sponsor	Q-CERT
Bronze Sponsor	HITACHI
Bronze Sponsor	PATCHLINK securing the enterprise
Daily Global Security News Podcast Sponsor	SecurityProPortal.com
Conference Program Coordination & USB Stick Sponsor	E-SECURE-IT ALERT & EARLY WARNING SYSTEM www.e-secure-it.com
Conference Program Coordination Sponsor	pentest security assurance
Ice Breaker Reception Sponsor	Juniper Networks
Vendor Display & Beer 'n Gear Sponsor	assuria
Vendor Display & Beer 'n Gear Sponsor	matta
Vendor Display & Beer 'n Gear Sponsor	SELEX Communications A Finmeccanica Company
Vendor Display	BorderWare
Vendor Display	endeavor security, inc.
Polo Shirt Sponsor	Sun microsystems
Bags Sponsor	Panda Software
T-shirt Sponsor	Google
Conference Folder Sponsor	Team Cymru www.cymru.com
Lanyard/Badge Sponsor	BFK
USB Stick Sponsor	KrCERT/CC Korea Internet Security Center
Security Challenge sponsor	S21sec

Conference program & room allocation

Saturday, June 16th

09:00 – 10:50	**Workshop** Train the Trainers Workshop (members only)
10:50 – 11:20	Morning Tea Break
11:20 – 13:10	Train the Trainers Workshop (continued)
13:10 – 14:40	Lunch Break
14:40 – 16:30	Train the Trainers Workshop (continued)
16:30 – 17:00	Afternoon Tea Break
17:00 – 18:50	Train the Trainers Workshop (continued)
	Arenal I & II

Sunday, June 17th

09:00 – 10:50	**Workshop** Train the Trainers Workshop (members only)
10:50 – 11:20	Morning Tea Break
11:20 – 13:10	Train the Trainers Workshop (continued)
13:10 – 14:40	Lunch Break
14:40 – 16:30	Train the Trainers Workshop (continued)
16:30 – 17:00	Afternoon Tea Break
17:00 – 18:50	Train the Trainers Workshop (continued)
	Arenal I & II
17:00 – 18:50	Program Committee Meeting
	Meet at Conference Reception Desk
19:00 – 21:00	**Welcome Ice Breaker Reception** Sponsored by Juniper Networks
	Santa Cruz

FIRST
Improving Security Together

June 17–22, 2007
Melia Sevilla Hotel
Seville, Spain

Last updated: June 21st, 2007

SEVILLE JUNE2007 SPAIN
19th Annual **FIRST** Conference

Monday, June 18th

09:00 – 10:50	**Tutorial** Creating and Managing CSIRTs *Georgia Killcrece and Robin Ruefle (CERT/CC, US)*	**Tutorial** Understanding & Analyzing Botnets *Jose Nazario and Jeff Nathan (Arbor Networks, US)*	**Geek Zone** Forensic Discovery *Dr. Wietse Z. Venema (IBM Research – GSAL, US)*	**SIG Meetings** Law Enforcement/ CSIRT Cooperation SIG *2nd LE CSIRT Cooperation Workshop*
10:50 – 11:20	Morning Tea Break			
11:20 – 13:10	Creating and Managing CSIRTs (continued)	Understanding & Analyzing Botnets (continued)	Forensic Discovery (continued)	Law Enforcement/ CSIRT Cooperation (continued)
13:10 – 14:40	Lunch Break			
14:40 – 16:30	Creating and Managing CSIRTs (continued)	Understanding & Analyzing Botnets (continued)	UNIX/C Programming traps and pitfalls *Dr. Wietse Z. Venema (IBM Research – GSAL, US)*	Internet Infrastructure Vendors (Vendor SIG) *Gaus (Cisco Systems, US)*
16:30 – 17:00	Afternoon Tea Break			
17:00 – 18:50	Creating and Managing CSIRTs (continued)	Understanding & Analyzing Botnets (continued)	UNIX/C Programming traps and pitfalls (continued)	Internet Infrastructure Vendors (Vendor SIG) (continued)
	Conference Room I – Giralda I & II	Conference Room II – Santa Cruz	Geek Zone Room I – Nervion I & II	SIG Room – Giralda III
19:00 – 22:00	**Beer 'n Gear**			Giralda IV & V
20:00 – 22:00	**FIRST Football Cup**			

Tuesday, June 19th

09:00 – 10:50	**Tutorial** Creating, Managing and Using a Malware Lab *Grant Deffenbaugh, Lisa Sittlerl and Nick Ianelli (CERT/CC, US)*	**Tutorial** System, Network and Security Log Analysis for Incident Response *Anton Chuvakin (LogLogic, Inc., US)*	**Tutorial** Windows Memory Forensics *Andreas Schuster (Deutsche Telekom AG, Group Security, DE) and Pär Österberg (Swedish IT Incident Centre, Sitic, SE)*	**Corporate Executive Programme (CEP)**
10:50 – 11:20	Morning Tea Break			
11:20 – 13:10	Creating, Managing and Using a Malware Lab (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Windows Memory Forensics (continued)	Common Vulnerability Scoring System SIG *Gavin Reid (Cisco Systems, US)*
13:10 – 14:40	Lunch Break			
14:40 – 16:30	Creating, Managing and Using a Malware Lab (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Windows Memory Forensics (continued)	T-ISAC Tech SIG *Peter G. Allor (ISS – Internet Security Systems, US)*
16:30 – 17:00	Afternoon Tea Break			
17:00 – 18:50	Creating, Managing and Using a Malware Lab (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Windows Memory Forensics (continued)	**SIG Meetings**
	Conference Room I – Giralda I & II	Conference Room II – Santa Cruz	Geek Zone Room I – Nervion I & II	SIG Room – Giralda III
19:00 –	**Pre AGM**			Santa Cruz

2nd LE CSIRT Cooperation Workshop

09:00 – 09:10	Opening *Howard Lamb (G8, UK-SOCA, UK) and Yurie Ito (FIRST, JPCERT/CC, JP)*
09:10 – 09:30	Working Together to Reduce Harm *Howard Lamb (SOCA, UK)*
09:30 – 09:50	Forensics Techniques and Tools *Dan Haagman (7Safe, UK)*
10:00 – 10:20	Forensics Techniques and Tools *Gary Dagan (FBI, US)*
10:30 – 10:50	Network forensics data for law enforcement investigations: What CSIRT should prepare *Ryan Connelly (Team Cymru, US)*
10:50 – 11:20	Morning Tea Break
11:20 – 11:40	Digital Forensics cooperation with Law Enforcement *Matthew (AusCERT, Australia)*
11:50 – 12:10	Analysis data supporting the efforts of Law Enforcement *Nicholas Ianelli, (CERT/CC, US)*
12:10 – 12:30	To be announced
12:30 – 13:10	Communication Protocol Discussion *lead by Howard Lamb (G8, UK-SOCA, UK), Mattew Pemble (Vizuri Limited, UK)*

Wednesday, June 20th

09:00 – 09:10	**Conference Opening**				
09:10 – 09:20	**Opening Speech**				
09:20 – 10:00	**Keynote Speaker:** *Lord Toby Harris of Haringey (House of Lords, UK)*				
10:00 – 10:50	Identity Management Systems: the forensic dimension *Peter Sommer (London School of Economics, UK)*	Data on Data Breaches: Past, Present, and Future *Adam Shostack and Chris Walsh (US)*	Long term instability of high priority incident response – A system dynamics simulation approach *Johannes Wiik, Jose Gonzalez (Agder University, NO) and Klaus-Peter Kossakowski (Presecure Consulting GmbH, DE)*	**Geek Zone** A day in the life of a hacker... Things we get up to when nobody is looking, and that keep me awake at night *Adam Laurie (The Bunker Secure Hosting Ltd., UK)*	**SIG Meetings** Network Monitoring SIG *Carol Overes, Menno Muller (GOVCERT.NL, NL)*
10:50 – 11:20			Morning Tea Break		
11:20 – 12:20	How many RAT's do you know? *Simon Gunning (Digilog UK Limited, UK)*	Inside the Perimeter: 6 Steps to Improve Your Security Monitoring *Chris Fry and Martin Nystrom (Cisco Systems, US)*	What We Learn From Cyber Exercises, or Not *James N. Duncan (Independent Consultant, US)*	A day in the life of a hacker... Things we get up to when nobody is looking, and that keep me awake at night (continued)	Network Monitoring SIG (continued)
12:20 – 13:10	Provider Practicalities and Paranoia: Modern ISP incident response *Scott McIntyre (KPN-CERT, NL)*	Taming Packets: The Network Expect Framework for Building Network Tools *Eloy Paris (Cisco PSIRT, US)*	Why Protection against Viruses, Bots, and Worms is so hard - Malware seen as Mobile Agents *Till Dörges (Presecure Consulting GmbH, DE)*		
13:10 – 14:40			Lunch Break		
14:40 – 15:40	Using Intelligence to Forecast Risk and Allocate Resources: It's Not Hocus-Pocus Anymore *Peter G. Allor (IBM ISS, US)*				
15:40 – 16:30	The Art of RFID Exploitation *Melanie Rieback (Vrije Universiteit Amsterdam, NL)*	Reviewing the VoIP Threat Landscape Peter Cox (Borderware, UK)	Security Risk Management: breaking through technology and market barriers – a real life story *Avi Corfas Skybox Security, US)*	**Geek Zone** Insider Threat – The Visual Conviction *Raffael Marty (ArcSight, Inc., US)*	CSIRT Metrics *Georgia Killcrece (CERT/CC – Carnegie Mellon University, US)*
16:30 – 17:00			Afternoon Tea Break		
17:00 – 18:00	Beyond the CPU: Defeating Hardware Based RAM Acquisition Tools *Joanna Rutkowska (Invisible Things Lab, PL)*	Cyber Fraud Trends and Mitigation *Ralph Thomas (Verisign/iDefense, US)*	Assessing Incident Severity in a Network and Automatic Defense Mechanisms *Klaus-Peter Kossakowski, Luis Francisco Servin Valencia and Till Dörges (Presecure Consulting GmbH, DE)*	Insider Threat – The Visual Conviction (continued)	CSIRT Metrics (continued)
18:00 – 18:50					
	Conference Room I – Giralda I & II	Conference Room II – Santa Cruz	Conference Room III – Arenal I	Geek Zone Room I – Nervion I & II	SIG Room – Giralda III

Conference Banquet: Hacienda El Visir
Buses will depart from the front of the hotel at 19:30

FIRST™
Improving Security Together

June 17–22, 2007
Melia Sevilla Hotel
Seville, Spain

Last updated: June 21st, 2007

SEVILLE JUNE2007 SPAIN
19th Annual **FIRST** Conference

Thursday, June 21st

09:00 – 09:10	Day Opening					
09:10 – 10:00	**Keynote Speaker:** *Francisco García Morán (Director General, DG Informatics, European Commission, EU)*					
10:00 – 10:50	Targeted attacks (spear phishing): A demonstration and analysis of a former Office 0-day vulnerability *Robert Hensing (MSCERT – Microsoft, US)*	Software Security: Integrating Security Tools Into a Secure Software Development Process *Kenneth van Wyk (KRvW Associates, LLC, US)*	Forensics for Managers –Presenting and understanding forensics from the MBA point of view *Mr. Ryan Washington, (Crucial Security, US)*	**Geek Zone** I know what you (and your company) did last summer... *Roelof Temmingh (Paterva, ZA)*	**Geek Zone** Botnet: Creation, usage , detection and eradication *Francisco Monserrat (IRIS-CERT – RedIRIS, ES), Guilherme Vênere and Jacomo Piccolini (CAIS/RNP, BR)*	**SIG Meetings**
10:50 – 11:20	Morning Tea Break					
11:20 – 12:20	The Security needs of the State versus the rights of the individual *Bob Ayers (Chatham House, UK)*	Flaws and frauds in the evaluation of IDS/IPS technologies *Stefano Zanero (Politecnico di Milano T.U. & Secure Network S.r.l., IT)*	NUS IT Security Landscape *Fong Lian Yong (National University of Singapore, SG)* Privacy matters in directories *Javier Masa, Jose Alfonso Accino and Victoriano Giralt (University of Malaga, ES)*	I know what you (and your company) did last summer... (continued)	Botnet: Creation, usage , detection and eradication (continued)	Abuse Handling (AH-SIG) *Martijn van der Heide (KPN-CERT, NL)*
12:20 – 13:10	Our Own Worst Enemies *Frank Wintle (PanMedia Ltd, UK)*	Vulnerability Remediation Decision Assistance system *Art Manion, Hal Burch (CERT/CC, US) and Yurie Ito (JPCERT/CC, JP)*	Dealing with Unreliable Software: Exile, Jail, and other Sentences *Bernd Grobauer, Heiko Patzlaff and Martin Wimmer (Siemens-CERT, DE)* Using instrumented browser instances for detecting 0-day exploits and filtering web traffic *Heiko Patzlaff (Siemens-CERT, DE)*			
13:10 – 14:40	Lunch Break					
14:40 – 15:40	**Keynote Speaker:** *George Stathakopoulos (General Manager of Product Security, Microsoft, US)*					
15:40 – 16:30	The Benefits of FIRST: How to sell FIRST to your Upper Management *Ray Stanton (BT, UK)*					
16:30 – 17:00	Afternoon Tea Break					
17:00 – 18:50	**Annual General Meeting (AGM)** Limited to FIRST team members, FIRST liaison members and their invited guests, subject to approval by the Steering Committee					
	Conference Room I – Giralda I & II	Conference Room II – Santa Cruz	Conference Room III – Arenal I	Geek Zone Room I – Nervion I & II	Geek Zone Room II – Arenal/Nervion III	SIG Room – Giralda III
19:00 – 21:00	**Sponsor Reception**	**Birds of a Feather (BOF)**				
	Terrace					

Friday, June 22nd

09:00 – 09:10	Day Opening					
09:10 – 10:00	**Keynote Speaker:** *Andrea Pirotti (Executive Director, ENISA, EU)*					
10:00 – 10:50	Building a scalable, accurate, actionable Incident Response system *Dr. Ken Baylor (CISSP CISM, VP & CISO Symantec, US)*	Electronic Forensics: A Case for First Responders *Henry Wolfe (University of Otago, NZ)*	Technical Evolution of Cybercrime *Rolf Schulz (ComCERT, DE)*	**Geek Zone** Tools and techniques to automate the discovery of zero day vulnerabilities *Joe Moore and Mark Rowe (Pentest Ltd, UK)*	**Geek Zone** Espionage – Reality or Myth? A Demonstration of Bugging Equipment *Emma Shaw (Esoteric Ltd, UK)*	**SIG Meetings**
10:50 – 11:20	Morning Tea Break					
11:20 – 12:20	SafeSOA: Managing Privacy & Risk In The Global Service Oriented Environment *Hart Rossman (SAIC, US)*	Handling Less-Than-Zero-Day Attack – A Case Study *Ma Huijuan (National University of Singapore, SG)* Setting up a Grid-CERT – Experiences of an academic CSIRT *Klaus Möeller (DFN-CERT, DE)*	An Internet Threat Evaluation Method based on Access Graph of Malicious Packets *Masaki Ishiguro and Hironobu Suzuki (Mitsubishi Research Institute, Inc., JP)*	Tools and techniques to automate the discovery of zero day vulnerabilities (continued)	Espionage – Reality or Myth? A Demonstration of Bugging Equipment (continued)	First Team Members Update Panel *Francisco (Paco) Monserrat (IRIS-CERT – RedIRIS, ES)*
12:20 – 13:10	New Trends and technologies in Identity Theft *Christoph Fisher (BFK Edv-Consulting Gmbh, DE)*	Unique Challanges for Incident Response in a Grid Environment *James Barlow (NCSA-IRST, US)*	The Evolution of Online Fraud *David Barroso (S21sec, ES)*			
13:10 – 14:40	Lunch Break					
14:40 – 15:40	**Keynote Speaker:** *Graham Whitehead (Futurologist, BT, UK)*					
15:40 – 16:30	WiMAX: Security Analysis and Experience Return *Laurent Butti (France Telecom Orange, FR)*	Developing a trusted partnership to prepare a framework for the collection of information security data *Carsten Casper (ENISA)*	Experiences with Building, Deploying and Running remote-controlled easily installable Network Sensors *Bernd Grobauer (Siemens CERT, DE)* Malware distribution trough software piracy: a case study *Jacomo Piccolini (CAIS/RNP, BR)*	Provider practicalities and paranoia: Modern ISP incident response – the tooling of incident response at a ISP *Scott McIntyre (KPN-CERT, NL)*	Identity theft in the corporate environment – demonstration and hands-on *Peter Wood (First Base Technologies, UK)*	Artifact Analysis (AA-SIG) *Kevin Houle (CERT/CC, US)*
16:30 – 17:00	Afternoon Tea Break					
17:00 – 17:45	Managing Privacy in Network Operations: Learning from the Law *Andrew Cormack, UK*	Tunisia's experience in establishing the first public CSIRT in Africa *Nabil Sahli (CERT-TCC, TN)* Setting up a governmental CERT: The CCN-CERT case study *Carlos Abad (CCN-CERT, ES)*		Provider practicalities and paranoia: Modern ISP incident response – the tooling of incident response at a ISP (continued)	Identity theft in the corporate environment – demonstration and hands-on (continued)	Artifact Analysis (AA-SIG) (continued)
17:45 – 18:00	How to Join FIRST *Damir (Gaus) Rajnovic (Cisco PSIRT – Cisco Systems Co., UK)*					
18:00 – 18:15	**Conference Closing**					
	Conference Room I – Giralda I & II	Conference Room II – Santa Cruz	Conference Room III – Arenal I	Geek Zone Room I – Nervion I & II	Geek Zone Room II – Arenal/Nervion III	SIG Room – Giralda III